Nama: Join Valentino Tampubolon

Kelas: B

NPM : 140810190020

Affine Cipher

Mis:

$$Key - 1 (a) = 3$$

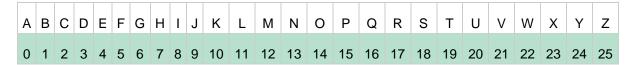
$$Key - 2 (b) = 2$$

Teks (x) = "masuk ke dalem keluar"

Enkripsi

Rumus: $C = ax + b \mod 26$

kita masih menggunakan susunan alpabet pada bagian dibawah ini.



Maka hasil yang kita dapatkan

- C[0] = 3(12) + 2 mod 26 = 12 = M
- $C[1] = 3(0) + 2 \mod 26 = 2 = C$
- C[2] = 3(18) + 2 mod 26 = 4 = E
- $C[3] = 3(20) + 2 \mod 26 = 10 = K$
- C [4] = 3(10) + 2 mod 26 = 6 = G
- $C[5] = 3(10) + 2 \mod 26 = 6 = G$
- $C[6] = 3(4) + 2 \mod 26 = 14 = 0$
- $C[7] = 3(3) + 2 \mod 26 = 11 = L$
- C[8] = 3(0) + 2 mod 26 = 2 = C
- $C[9] = 3(11) + 2 \mod 26 = 9 = J$
- $C[10] = 3(4) + 2 \mod 26 = 14 = 0$
- C [11] = 3(12) + 2 mod 26 = 12 = M
- $C[12] = 3(10) + 2 \mod 26 = 6 = G$
- C [13] = 3(4) + 2 mod 26 = 14 = 0
- $C[14] = 3(11) + 2 \mod 26 = 9 = J$
- C[15] = 3(20) + 2 mod 26 = 10 = K
- $C[16] = 3(0) + 2 \mod 26 = 2 = C$

```
- C[17] = 3(17) + 2 \mod 26 = 1 = B
```

Dekripsi

Rumus : $P = a^{-1} (x - b) \mod m$

Pertama kita harus mengetahui a-1 dimana harus memenuhi

 $a^{-1} \mod m = 1$

GCD(3,26)

$$26 = 3*8 + 2$$

$$3 = 2*1 + 1$$

$$2 = 1*2 + 0$$

$$t0 = 0$$
 $t1 = 1$

$$q1 = 8 q2 = 1 q3 = 2$$

$$t2 = (0 - (8.1)) \mod 26 = -8 \mod 26 = 18$$

$$t3 = (1 - (1.18)) \mod 26 = -17 \mod 26 = 9$$

$$a^{-1} = 9$$

Lalu kita lakukan dekripsi "DSAPHCMVKFSJSP" sesuai dengan rumus yang ada:

- $C[0] = 9(12 2) \mod 26 = 12 = M$
- $C[1] = 9(2 2) \mod 26 = 0 = A$
- C[2] = 9(4 2) mod 26 = 18 = S
- $C[3] = 9(10 2) \mod 26 = 20 = U$
- C[4] = 9(6 2) mod 26 = 10 = K
- C[5] = 9(6 2) mod 26 = 10 = K
- $C[6] = 9(14 2) \mod 26 = 4 = E$
- C [7] = 9(11 2) mod 26 = 3 = D
- $C[8] = 9(2-2) \mod 26 = 0 = A$
- $C[9] = 9(9 2) \mod 26 = 11 = L$
- $C[10] = 9(14 2) \mod 26 = 4 = E$
- $C[11] = 9(12 2) \mod 26 = 12 = M$
- $C[12] = 9(6-2) \mod 26 = 10 = K$
- C [13] = 9(14 2) mod 26 = 4 = E
 C [14] = 9(9 2) mod 26 = 11 = L
- C [15] = 9(10 2) mod 26 = 20 = U
- $C[16] = 9(2-2) \mod 26 = 0 = A$
- $C[17] = 9(1-2) \mod 26 = 17 = R$

Maka, hasil akhirnya sesuai dengan plainteks.